Міністерство освіти і науки України

Національний університет водного господарства та природокористування

Навчально-науковий інститут автоматики, кібернетики та обчислювальної техніки

Кафедра обчислювальної техніки

04-04-10

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної, методичної та виховної роботи
_____ Лагоднюк О.А.
“__” _____ 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline
Основи теорії захисту інформації

Fundamentals of the theory of information security in computer systems

---

спеціальність	**123 "Комп’ютерна інженерія"**
specialty	**123 Computer Engineering**

Рівне – 2018

Робоча програма навчальної дисципліни «Основи теорії захисту інформації» для здобувачів вищої освіти другого (магістерського) рівня галузі знань 12 «Інформаційні технології» за спеціальністю 123 "Комп'ютерна інженерія". Рівне: НУВГП, 2018. – 17 с.

Розробник: Назарук Віталій Дмитрович, ст. викладач кафедри обчислювальної техніки, к.т.н

Робочу програму схвалено на засіданні кафедри обчислювальної тех-ніки. Протокол від " 07 " вересня 2018 року № 1.
Завідувач кафедри _____ Б.Б. Круліковський

Схвалено науково-методичною комісією за спеціальністю 123 "Комп'ютерна інженерія". Протокол від "10" вересня 2018 року № 1
Голова науково-методичної комісії _____ М.Т. Соломко

ВСТУП

Програма нормативної навчальної дисципліни "Основи теорії захисту інформації " складена на підставі навчального плану для здобувачів вищої освіти другого (магістерського рівня). Предметом вивчення навчальної дисципліни є формування у студентів теоретичних знань і розуміння принципів побудови систем технічного та криптографічного захисту інформації в комп'ютерних системах, а також практичних навичок по виявленню технічних каналів витоку інформації та способів несанкціонованого доступу. Опанування основних положень зазначеного курсу передбачає наявність міждисциплінарних зв'язків таких дисциплін, як "Теорія інформації", "Архітектура комп'ютера", «Захист інформації в комп'ютерних системах», «Теорія електричних та магнітних кіл». На матеріалі даної дисципліни може ґрунтуватись вивчення наступних професійно спрямованих дисциплін: "Технологія проектування комп'ютерних систем", "Комп'ютерні системи".

Анотація

Навчальний курс призначений для вивчення основ теорії захисту інформації в комп'ютерних системах, в якому викладено загальні підходи та класифікація загроз для інформації щодо цілісності, конфіденційності та спостережності, методів та засобів їх локалізації та блокування. Подано принципи побудови систем технічного та криптографічного захисту інформації. Приведено описи та розглянуто функціонал сучасних криптоалгоритмів, функцій хешування та електронного цифрового підпису.

Ключові слова: технічні канали витоку інформації, небезпечний сигнал, контрольована зона, симетричні криптоалгоритми, асиметричні криптоалгоритми, електронний цифровий підпис.

Abstract

The training course is designed to study the foundations of the

theory of information security in computer systems, which outlines common approaches and the classification of threats for information on integrity, confidentiality and observation, methods and tools for their localization and blocking. The principles of construction of technical and cryptographic information security systems are presented. The given descriptions describe the functional of modern cryptographic algor-?thms, hashing functions and electronic digital signature.

Key words: technical channels of information leakage, hazardous signal, controlled zone, symmetric cryptographic algorithms, asymmetric cryptographic algorithms, electronic digital signature.

1. **Опис навчальної дисципліни**

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма</td><td>заочна форма</td></tr>
<tr><td>Кількість кредитів – 4,5</td><td>Галузь знань
12 Інформаційні технології</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="3">Спеціальність
123 "Комп’ютерна інженерія"</td><td colspan="2">Рік підготовки</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>5-й</td><td>5-й</td></tr>
<tr><td rowspan="3">Спеціалізація
"Комп’ютерні системи
та компоненти"</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 135</td><td>9-й</td><td>9-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="3">Тижневих годин для денної форми навчання:</td><td rowspan="3">Рівень вищої світи:
2 магістерський</td><td>24 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>24 год.</td><td>8 год.</td></tr>
</table>

аудиторних – 4 самостійної роботи –7		Самостійна робота	
		91 год.	119 год.
		Індивідуальні завдання:	
		Форма контролю:	
		іспит	

Примітка. Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання –34/ 66%

для заочної форми навчання – 12/ 88 %.

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни є набуття теоретичних знань та практичних навичок побудови систем технічного та криптографічного захисту інформації на основі розроблених моделей загроз.

Завданням дисципліни є:

- формування системного підходу до дослідження систем технічного та криптографічного захисту інформації в комп'ютерних системах;
- набуття навиків розроблення моделі загроз та моделі порушника інформаційно-комп'ютерних систем;
- отримання знань порядку застосування існуючих та перспективних технологій захисту інформації.

В результаті вивчення дисципліни студенти повинні

знати:

- види загроз для інформації в комп'ютерних системах, їх класифікацію та наслідки реалізації;
- теоретичні основи техніічних каналів витоку інформації, способи їх локалізації на об'єктах інформаційної діяльності;
- принципи роботи сучасних симетричних та асиметричних криптоалгоритмів;
- порядок формування електронного цифрового підпису.

вміти:

- виконувати моніторинг процесів функціонування комп'ютерних

мереж та інформаційно-телекомунікаційних систем в умовах реалізації загроз різних класів та впливів зовнішніх дестабілізуючих факторів з метою зменшення їх впливу на процеси обміну даними;
- застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;
- забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановлено політики безпеки.

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1. Загрози для інформації в комп'ютерних системах. Технічний захист інформації.

Тема № 1: Визначення інформації. Загрози для інформації. Основні види розвідки. Класифікація зловмисників комп'ютерних систем

Тема № 2: Класифікація і структура технічних каналів витоку інформації. Модель технічного каналу витоку інформації. Засоби технічної розвідки

Тема № 3: Технічні канали витоку інформації. Фізичні основи побічних електромагнітних випромінювань. Електрична складова. Магнітна складова. Спектральна характеристика побічних електромагнітних випромінювань.

Тема № 4: Технічні методи і засоби захисту інформації. Організація захисту від технічних каналів витоку інформації. Порядок виявлення та локалізація портативних електронних пристроїв перехоплення інформації.

Тема № 5: Методи та засоби несанкціонованого доступу до інформації. Фізичні та логічні способи несанкціонованого доступу. Активні та пасивні форми несанкціонованого доступу.

Тема № 6: Програмні засоби захисту інформації. Засоби захисту операційних систем. Надбудовані комплекси засобів захисту.

Модуль 2.

Змістовий модуль 2. Криптографічний захист інформації. Основи криптоаналізу.

Тема № 7: Історія криптографії. Математичні основи шифрування. Докомп'ютерні криптоалгоритми. Принципи побудови та технічної реалізації.

Тема № 8: Мережа Фейстеля. Конструкція, модифікації. Симетричні криптоалгоритми на основі мережі Фейстеля. Криптоалгоритм DES, Структура та принцип дії.

Тема № 9: Симетричний криптоалгоритм ГОСТ 38147-89, конструкція, принцип дії. Криптоалгоритми на основі схеми Лей-Мессі Вітчизняний криптоалгоритм «Калина», особливості побудови.

Тема № 10: Асиметричні криптоалгоритми. Одностороння функція. Алгоритм Діффі-Хелмана. Криптоалгоритм RSA,

Тема № 11: Хеш-функції, конструкція, принцип дії. Електронний цифровий підпис, особливості побудови, організації застосування та сертифікації

Тема № 12: Основи криптоаналізу. Основні прийоми та алгоритми.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	всього	у тому числі				всього	у тому числі			
		лекції	лаборат.	індівід..	с. р.с.		лекції	лаборат.	індівід..	с. р.с.
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
Модуль 1										
Змістовий модуль 1. Загрози для інформації в комп'ютерних системах. Технічний захист інформації.										
Тема 1. Визначення інформації. Загрози для інформації. Основні види розвідки. Класифікація зловмисників комп'ютерних систем	11	2			9	11				11
Тема 2. Класифікація і структура технічних каналів витоку інформації	11	2	2		7	11				11
Тема 3. Технічні канали витоку інформації. Фізичні основи побічних електромагнітних випромінювань	11	2	2		7	11	2	2		7
Тема 4. Технічні методи і засоби захисту інформації.	11	2	2		7	11				11

Тема 5. Методи та засоби несанкціонованого доступу до інформації	11	2	2		7	11				11
Тема 6. Програмні засоби захисту інформації.	14	2	6		6	14	2	4		8
Разом за змістовим модулем 1	69	12	14		43	69	4	6		59
Модуль 2										
Змістовий модуль 2. Криптографічний захист інформації. Основи криптоаналізу										
Тема № 7: Історія криптографії. Математичні основи шифрування. Ручні криптоалгоритми	11	2	2		7	11				11
Тема № 8: Мережа Фейстеля. Симетричний криптоалгоритм DES.	11	2	2		7	11	2	2		9
Тема № 9: Симетричний криптоалгоритм ГОСТ 38147-89. Криптоалгоритм «Калина».	11	2	2		7	11		2		9
Тема № 10: Алгоритм Діффі-Хелмана. Асиметричні криптоалгоритми.	11	2	2		7	11				11
Тема № 11: Хеш-функції. Електронний цифровий підпис.	11	2	2		7	11				11
Тема № 12: Основи	11	2			9	11				11

криптоаналізу.										
Разом за змістовим модулем 2	66	12	10		44	77	2	4		62
Усього годин	135	24	24		87	135	6	8		121
Разом	135	24	24		87	135	6	8		121

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	ЛР №1. Визначення амплітуди гармонік та побудова спектра побічних електромагнітних випромінювань монітора комп'ютера.	2	
2	ЛР №2. Створення просторового широкосмугового шумового сигналу для захисту комп'ютера від витоку інформації за рахунок побічних електромагнітних випромінювань.	2	
3	ЛР № 3 Дослідження політики облікових записів ОС WINDOWS XP.	2	2
4	ЛР № 4 Вивчення функціональних характеристик комплексу засобів захисту «Гриф-ХР».	2	
5	ЛР № 5. Інсталяція комплексу засобів захисту «Гриф-ХР» на автоматизовану систему класу 1.	2	
6	ЛР № 6. Вивчення функціональних характеристик комплексу засобів захисту «Лоза»	4	4
7	ЛР № 7. Встановлення параметрів входу до системи. Встановлення параметрів захисту друку та експорту документів.	4	2
8	ЛР № 8. Встановлення параметрів ключових дисків. Блокування дисків.	2	
9	ЛР № 9. Встановлення параметрів заборони друку. Встановлення політики аудита	2	
10	ЛР № 10. Встановлення політики блокування	2	

	облікового запису. Встановлення політики паролів		
	Разом	24	8

6. Самостійна робота

За навчальним планом на самостійну роботу відводиться 87 година для студентів денної форми навчання та 121 годин для студентів заочної форми навчання.

Самостійна робота студента включає наступні види робіт:

- самостійне опрацювання лекційного матеріалу з кожної теми;
- підготовка до виконання лабораторних робіт;
- обробка результатів досліджень, оформлення звітів, підготовка та захист лабораторних робіт;
- підготовка до модульних контрольних робіт (тестування);
- виконання індивідуального навчально-дослідного завдання (курсової роботи);
- підготовка до підсумкового контролю (іспит).

6.1 Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Загрози для інформації. Основні види розвідки. Класифікація зловмисників комп'ютерних систем	5	7
2	Класифікація і структура технічних каналів витоку інформації	9	11
3	Технічні канали витоку інформації. Фізичні основи побічних електромагнітних випромінювань	7	9
4	Методи та засоби несанкціонованого доступу до інформації	7	11
5	Технічні методи і засоби захисту інформації.	9	11
6	Програмні засоби захисту інформації.	5	5

7	Математичні основи шифрування. Ручні криптоалгоритми.	7	10
8	Мережа Фейстеля. Симетричний криптоалгоритм DES.	5	10
9	Симетричний криптоалгоритм ГОСТ 38147-89. Криптоалгоритм «Калина».	9	9
10	Алгоритм Діффі-Хелмана. Асиметричні криптоалгоритми.	9	9
11	Хеш-функції.	5	10
12	Електронний цифровий підпис.	7	9
13	Основи криптоаналізу.	7	10
	Разом	87	121

7. Індивідуальне навчально-дослідне завдання

Не передбачено

8. Методи навчання

Лекційні заняття проводяться з використанням проектора, переносних комп'ютерів викладача та студентів Завдання лабораторних робіт передбачають, в тому числі, виконання завдань учбово-дослідного характеру з частково невизначеними умовами.

9. Методи контролю

Для поточного контролю знань студентів з навчальної дисципліни використовуються такі методи:

- на лекційних заняттях проводиться контроль присутності студентів та контроль якості конспектів лекцій;
- на лабораторних заняттях проводиться контроль готовності до заняття шляхом тестового експрес-опитування, а також шляхом захисту звітів з лабораторної роботи у вигляді співбесіди;
- контроль самостійної роботи проводиться у вигляді співбесіди на задану тему;
- оцінка модульних контрольних робіт (тестування);
- підсумковий контроль проводиться в кінці семестра у вигляді іспиту.

Усі форми контролю включено до 100-бальної шкали оціню-

вання.

Оцінювання результатів поточної роботи (завдань, що виконуються на лабораторних заняттях, результати самостійної роботи студентів) проводиться за такими критеріями:

Лабораторні роботи (у % від кількості балів, виділених на завдання із заокругленням до цілого числа):

0 % – завдання не виконано;

40% – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру;

60% – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці;

80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

100% – завдання виконано правильно, вчасно і без зауважень.

10. Розподіл балів, що отримують студенти

Поточне тестування та самостійна робота												Підсумковий тест (іспит)	Сума
Змістовий модуль 1						Змістовий модуль 2						40	100
T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}		
5	5	5	5	5	5	5	5	5	5	5	5		

T_1, T_2 ... T_{18} – теми змістових модулів.

Шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсового проекту (роботи)	для заліку
90-100	відмінно	зараховано
82-89	добре	
74-81		
64-73	задовільно	
60-63		
35-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11. Методичне забезпечення

1. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни "Основи теорії захисту інформації» 12 "Інформаційні технології" денної та заочної форм навчання /Назарук В.Д. - Рівне: НУВГП. 2018. - 27 с. Електронний ресурс. Режим доступу http://ep3.nuwm.edu.ua/id/eprint /7327/

12. Рекомендована література

Базова

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации . Том 1. Несанкционированное получение информации Киев: Арий 2008, 326с.

2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации . Том 2. Информционная безопасность Киев: Арий 2008 385с.

3. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах Харьков: СМИТ 2010 465с.

4. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.

5. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

Допоміжна

1. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил.

2. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Перевод В.Ф.Писаренко)

3. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энциклопедия компьютерных вирусов. - М.: «СОЛОН-Р», 2001.

4. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.- 2-е изд., перераб. и доп.-М.: Радио и связь, 2001.-376 с: ил.

5. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с

англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил.

6. Хорошков В. А., Чекатков А. А. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003.- 504с., ил.

7. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002.

13. Інформаційні ресурси

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР,. Режим доступу: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

2. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id=89734&ctime=1344500065981

3. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734

4. Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99. Режим доступу http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=251506&cat_id=89734&ctime=1462971480804

5. Положення про проведення відкритого конкурсу криптографічних алгоритмів. Державна служба спеціального зв'язку та захисту інформації Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/ru/publish/article;jsessionid=A5640057AD30A40EE74C44F1D5292735?art_id=48387&cat_id=103375